METHOD AND APPARATUS FOR ESTABLISHING A SHARED CRYPTOGRAPHIC KEY BETWEEN ENERGY-LIMITED NODES IN A NETWORK

ABSTRACT

One embodiment of the present invention provides a system for establishing a cryptographic key between energy-limited nodes using a super node that has abundant energy. The node also sends a message to a super node including the partial key value encrypted using the super node's a public key. Note that the energy-limited node only encrypts with the public key, which requires less energy than decrypting with the corresponding private key. The super node then decrypts to recover the partial key value. Next, the super node securely communicates the partial key value to the second node. The second node then establishes the cryptographic key using the first and second node's partial key values.